FITBIT DATA AND THE FOURTH AMENDMENT: WHY THE COLLECTION OF DATA FROM A FITBIT CONSTITUTES A SEARCH AND SHOULD REQUIRE A WARRANT IN LIGHT OF *CARPENTER V. UNITED STATES*

Alxis Rodis*

* JD Candidate, William & Mary Law School, 2021; BA, Dickinson College, 2018. First and foremost, I would like to thank my parents, Christina and Ricky. I would not be where I am today were it not for your unwavering and unconditional support of my goals. I would also like to thank Professor Doug Edlin for inspiring and believing in me; and Jake, for keeping me sane. Finally, I would like to thank the staff and editorial board of the *William & Mary Bill of Rights Journal* for their assistance throughout the publication process.

INTRODUCTION

As Justice Tom Clark once said, "We cannot forgive the requirements of the Fourth Amendment in the name of law enforcement."[1] As technology has increasingly become a part of our everyday lives, law enforcement officials often attempt to use the collection of metadata from technological devices, including fitness trackers such as Fitbits, to assist in their law enforcement endeavors.[2] In fact, today the government has numerous "sophisticated ways of seeing, hearing, and tracking people, ways that were unimaginable to the Fourth Amendment's Framers."[3]

For example, in 2015, Connie Dabate was murdered inside her home while wearing a Fitbit.[4] In the course of the investigation of her murder, her husband, Richard Dabate, told investigators that several masked intruders broke into their home and shot his wife at approximately 9:00 a.m.[5] However, after police collected data from his wife's Fitbit, they were able to determine that her last movements inside the home

---

[1] MIMI CLARK GRONLUND, SUPREME COURT JUSTICE TOM C. CLARK: A LIFE OF SERVICE 204 (2010).

[2] *See, e.g.*, Nicholas Rondinone, *Richard Dabate Rejects Plea Deal in Fitbit Murder Case, Pushes for Trial in Wife's Killing*, HARTFORD COURANT (Jan. 24, 2019, 5:10 PM), http://www.courant.com/breaking-news/hc-br-dabate-fitbit-murder-20190124-rmxjg4hwn5egzij3cesi3dd6ki-story.html [http://perma.cc/BP26-PUGV].

[3] Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 412.

[4] Dave Altimari, *All Evidence Turned over as Fitbit Murder Case Moves Toward Trial*, HARTFORD COURANT (July 20, 2018, 12:30 PM), http://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html [http://perma.cc/GE5B-V3GG].

[5] Rondinone, *supra* note 2; Gabriella Paiella, *A Dead Woman's Fitbit Data May Lead to Her Husband's Murder Conviction*, CUT (Apr. 25, 2017), http://www.thecut.com/2017/04/fitbit-murder-case-richard-dabate.html [http://perma.cc/9TM8-XGDT].

were actually not until 10:05 a.m., more than an hour after her husband stated that she had been murdered by unknown intruders.[6] As a result of this information and other circumstantial evidence,[7] Richard Dabate was charged with the first-degree murder of his wife.[8]

The Richard Dabate case demonstrates the potential use of Fitbit data in criminal prosecutions. In that case, Connie Dabate's Fitbit turned out to be the most valuable witness in the government's case against her husband.[9] Fitbits are commonly worn by individuals during all waking hours, and the devices track a large breadth of personal data, such as the number of steps the user takes each day, their total distance traveled, the number of calories burned, their weight, heart rate, average sleep stages, total active minutes, and even their location.[10] This data has the potential to reveal the intimacies of one's life, including daily whereabouts and sensitive health information.[11] Thus, because of the popularity of these devices in our modern world, the sensitive nature of the information stored on these devices and their potential use in criminal investigations and prosecutions, it is imperative to determine whether the collection of data from a Fitbit constitutes a search and, if so, whether such a search requires a warrant.

This Note will argue that, in light of the Supreme Court's recent decision in *Carpenter v. United States*, the collection of seven or more days of Fitbit data constitutes a search and, as such, requires the police to obtain a warrant before collecting such data.[12] Part I of this Note reviews the text of the Fourth Amendment and its requirements. Part II provides an overview the history of the Fourth Amendment doctrine and what constitutes a search under the Fourth Amendment. Part III analyzes the Supreme Court's decision in *Carpenter* and the implications of that case. Part IV provides information regarding Fitbits, the data they store, and their potential to be used in criminal prosecutions. Finally, Part V analyzes the *Carpenter* decision in the context of the collection of data from Fitbits to argue that such a collection of data constitutes a search and requires a warrant under the Fourth Amendment. It then proposes a rule for future cases that involve determining whether the collection of data constitutes a search.

---

[6] Rondinone, *supra* note 2.

[7] Altimari, *supra* note 4 (explaining that police gathered cellphone, text message, Facebook, and FitBit records for Connie Dabate as well as computer records from Richard Dabate's laptop).

[8] Paiella, *supra* note 5.

[9] Marguerite Reardon, *Your Alexa and Fitbit Can Testify Against You in Court*, CNET (Apr. 5, 2018, 5:00 AM), http://www.cnet.com/news/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court/ [http://perma.cc/UH48-PPUC].

[10] *Fitbit Privacy Policy*, FITBIT, http://www.fitbit.com/legal/privacy-policy [http://perma.cc/GZF9-FJUA] (last visited Dec. 8, 2020).

[11] *See id.*

[12] *See* 138 S. Ct. 2206, 2217 n.3 (2018).

I. THE FOURTH AMENDMENT

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The Fourth Amendment contains two primary requirements: the reasonableness requirement and the warrant requirement.[14] With respect to the reasonableness requirement, courts have long held that, according to the text of the Fourth Amendment, the "ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[15] Warrantless searches are considered per se unreasonable, subject only to a few, narrow exceptions.[16]

Because of the presumption under the Fourth Amendment that warrantless searches are unreasonable, the Supreme Court created the exclusionary rule to deter unlawful police conduct and encourage law enforcement officials to obtain a warrant prior to conducting a search of a constitutionally protected area.[17] Although the exclusionary rule is not written into the text of the Fourth Amendment itself, it has become a foundational principle of Fourth Amendment jurisprudence.[18] Justice Alito recently described the exclusionary rule as "a deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation."[19]

The exclusionary rule derives its origins from *Mapp v. Ohio*, a 1961 Supreme Court case involving the warrantless search of a woman's home.[20] In that case, police

---

[13] U.S. CONST. amend. IV.

[14] *See id.*

[15] William Kendall, Note, *"Outrunning" the Fourth Amendment: A Functional Approach to Searches of Wearable Fitness Tracking Devices*, 43 S. ILL. U. L.J. 333, 339 (2019) (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 652 (1995)).

[16] Katz v. United States, 389 U.S. 347, 357 (1967). Exceptions to the warrant requirement include searches conducted pursuant to consent, incident to a lawful arrest, pursuant to exigent circumstances (such as an imminent risk of destruction of evidence, an imminent danger to the community, or the hot pursuit of a suspect), and searches of objects in plain view. *See Fourth Amendment*, LEGAL INFO. INST., http://www.law.cornell.edu/wex/fourth_amendment [http://perma.cc/BG96-8VLU] (June 2017).

[17] *See* Alexandra Carthew, Comment, *Searches and Seizures—Fourth Amendment and Reasonableness in General: Protection of Privacy Interests in the Digital Age*, 94 N.D. L. REV. 197, 200–01 (2019).

[18] *See id.* at 200.

[19] *Id.* at 201 (quoting Davis v. United States, 564 U.S. 229, 231–32 (2011)).

[20] *See* 367 U.S. 643, 644–45 (1961).

arrived at Mapp's home in search of a suspect they believed was hiding inside.[21] When Mapp answered the door, she requested the police produce a warrant before she permitted them entry into the home.[22] The officers produced a piece of paper, which they handed to Mapp, and then proceeded to search the home, where they found and seized pornography.[23] Later, it was revealed that the piece of paper that officers had shown Mapp was not, in fact, a valid warrant, and, as such, the pornography seized was the result of an unlawful, warrantless search.[24] On appeal, the Supreme Court held that the exclusionary rule applied to the states through the incorporation of the Fourteenth Amendment, and thus, all evidence obtained by searches and seizures in violation of the Fourth and Fourteenth Amendments is inadmissible in state court.[25]

Together, the warrant requirement of the Fourth Amendment and the court-created exclusionary rule mean that any evidence obtained from a warrantless search cannot be used in a criminal prosecution.[26] Because of the importance of this default rule in determining the admissibility of evidence in criminal trials, this Note next examines what constitutes a "search" under the Fourth Amendment in order to clarify when the warrant requirement applies.

II. HISTORY OF THE "SEARCH" DOCTRINE

A. The Olmstead *Trespassory Doctrine*

Originally, the Fourth Amendment was understood to protect against *only* a physical trespass by a person into a constitutionally protected area.[27] In *Olmstead v. United States*, a 1928 Supreme Court case, the Court considered a Fourth Amendment challenge to evidence that was obtained via a wiretap.[28] In that case, Olmstead and his co-defendants were convicted of conspiring to violate the federal prohibition laws that

---

[21] *Id.* at 644.

[22] *Id.*

[23] *Id.* at 644–45.

[24] *Id.* at 645.

[25] *Id.* at 655.

[26] *See id.*; U.S. CONST. amend. IV.

[27] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928). The *Olmstead* Court stated:

> Neither the cases we have cited nor any of the many federal decisions . . . hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual *physical invasion* of his house "or curtilage" for the purpose of making a seizure.

Id. (emphasis added); *see also* Eunice Park, *Objects, Places and Cyber-Spaces Post-*Carpenter*: Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J.L. & TECH. 1, 8 (2019).

[28] 277 U.S. at 455–66.

were still in force at that time.[29] Wiretaps of the alleged conspirators' telephone conversations were the government's primary evidence used to establish the existence of the conspiracy.[30] The question before the Court was whether the use of wire tapping to obtain defendants' private telephone conversations constituted a violation of the Fourth Amendment.[31] The Court held that the wiretap was *not* a Fourth Amendment violation, explaining that such a violation could not exist without an actual search or seizure of a person or their material effects, or a physical invasion of a person's home.[32] Thus, because the wiretap was conducted *without* a physical trespass by the government, the Court held that the Fourth Amendment's protections were inapplicable.[33]

B. The Katz *Reasonable Expectation of Privacy Test*

The Supreme Court's interpretation of the Fourth Amendment remained closely related to concepts of property law until 1967, when the *Olmstead* trespassory doctrine was overruled by *Katz v. United States*.[34] *Katz* expanded the protection of the Fourth Amendment beyond merely guarding against physical intrusions.[35] Since then, the Supreme Court has continuously recognized a more expansive view of the Fourth Amendment's protections, encompassing not only the right to be free from physical trespass, but also the right to individual privacy.[36]

In *Katz*, FBI agents attached an electronic listening device to the outside of a public telephone booth.[37] When Katz entered the phone booth, the device was used to record his conversation.[38] As a result of the wiretap, Katz was convicted under an eight-count indictment charging him with transmitting illegal wagering information via telephone.[39] Both the district court and the court of appeals found that there had been no Fourth Amendment violation because the agents had not *physically* entered the phone booth, and, under *Olmstead*, absent a physical trespass, there could be no constitutional violation.[40] The Supreme Court reversed the decisions of the lower courts, reasoning that even though there had been no physical trespass, a person who enters a telephone booth and shuts the door behind him has a reasonable expectation

---

[29] *Id.* at 456–57.
[30] *Id.*
[31] *Id.* at 455.
[32] *Id.* at 466.
[33] *Id.*
[34] *See* 389 U.S. 347, 353 (1967).
[35] Carthew, *supra* note 17, at 201.
[36] *See id.*; Park, *supra* note 27, at 8.
[37] *Katz*, 389 U.S. at 348.
[38] *Id.*
[39] *Id.*
[40] *Id.* at 348–49.

that his communications would not be broadcast to the world, and such an expectation of privacy is protected under the Fourth Amendment.[41] As such, the Court held that the wiretap constituted a violation of Katz's Fourth Amendment protections.[42]

This more expansive view of Fourth Amendment coverage produced what has come to be known as the *Katz* reasonable expectation of privacy test.[43] The actual test is articulated in Justice Harlan's concurring opinion in *Katz*.[44] The test is comprised of two unique, but related, requirements: "[F]irst[,] that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[45] The Court also noted that once a reasonable expectation of privacy has been established, the burden then shifts to the government to justify the warrantless search.[46] The Court reasoned that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection[,] [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[47] Thus, the Supreme Court overruled the narrower *Olmstead* trespassory doctrine in favor of the idea that the Fourth Amendment governs not only the seizure of tangible items, but also extends to the recording of oral statements, overheard without any physical trespass.[48]

C. The Third-Party Doctrine

Although the *Katz* reasonable expectation of privacy test represents a relatively expansive view of Fourth Amendment protections, one notable limitation on such protection is the third-party doctrine.[49] According to this doctrine, the Fourth Amendment does not prohibit the government from obtaining information that an individual conveys to a third party, even if that information was originally given to the third

---

[41] *Id.* at 352. The Court stated:

> One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Id.

[42] *Id.* at 353.

[43] *See id.* at 361 (Harlan, J., concurring).

[44] *Id.*

[45] *Id.*

[46] *See id.* at 357 (majority opinion).

[47] *Id.* at 351–52 (citations omitted).

[48] *See id.* at 353. In *United States v. Jones*, the Court clarified that the *Katz* reasonableness test is not the *exclusive* test for determining Fourth Amendment violations. 565 U.S. 400, 411–12 (2012). Rather, the Court noted that it may better be understood as supplementing the default rule that when a classic, physical trespass is present, a Fourth Amendment violation has occurred. *See id.*

[49] *See* United States v. Miller, 425 U.S. 435, 443 (1976).

party with the assumption that it would only be used for a limited purpose and that it would not be exposed to others.[50]

The third-party doctrine originated in *United States v. Miller*, a Supreme Court case in which a defendant was convicted for operating an undocumented whiskey distillery in Georgia.[51] During their investigation of the case, the government obtained copies of checks and other financial records belonging to the defendant without a warrant.[52] However, the Court held that Miller had no legitimate expectation of privacy in the checks or financial records, as he had voluntarily conveyed this information to the bank and its employees—a third party.[53]

The Supreme Court later affirmed its reasoning from *Miller* in *Smith v. Maryland*.[54] In that case, a robbery victim called the police and reported that a man, identifying himself as the robber, had made numerous threatening phone calls to her in the days following the robbery.[55] During one of these calls, the man told the victim to step outside, and when the victim did so, she saw the man driving slowly past her home.[56] The government used the victim's reports to trace the license plate number of the robber's vehicle to a man named Michael Smith.[57] Subsequently, the government, without obtaining a warrant for Smith's phone records, directed Smith's telephone company to install a pen register that would record the numbers Smith dialed from his home.[58] The pen register revealed that Smith was in fact calling the victim.[59] Using this information, the government secured a search warrant for Smith's home that revealed evidence of the robbery.[60]

The result of the Supreme Court's holdings in *Smith* and *Miller* is a bright-line rule that an individual "has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[61] Accordingly, "the Government is typically free to obtain such information from [the third party] without triggering Fourth

---

[50] *Id.*

[51] *Id.* at 436–39.

[52] *Id.*

[53] *See id.* at 440, 442.

[54] *See generally* 442 U.S. 735 (1979).

[55] *Id.* at 737.

[56] *Id.*

[57] *Id.*

[58] *Id.* A pen register is a mechanical device that can be installed on a landline telephone to record the outgoing phone numbers dialed on the landline "by monitoring the electronic impulses caused when the dial on the telephone is released." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977). The device is not capable of recording the content of the communications via telephone, nor does it indicate whether the calls placed were actually completed. *Id.*

[59] *Smith*, 442 U.S. at 737.

[60] *Id.* (The search of Smith's home revealed that a page in his phone book was turned down to the name and number of Patricia McDonough, the victim of the robbery. Police seized the phone book, and Smith was later indicted for robbery.).

[61] *Id.* at 743–44 (citing United States v. Miller, 425 U.S. 435, 442–44 (1976)).

Amendment protections."[62] This rule rests on two main justifications. "[F]irst, since business records are not confidential communications, [a] defendant can 'assert neither ownership nor possession'" over such records.[63] Second, a defendant who voluntarily exposes or shares private information with another person or entity thereby forgoes any expectation of privacy he might have claimed in that information.[64]

Thus, the Supreme Court's doctrine regarding Fourth Amendment protections suggests that a person who has a reasonable expectation of privacy in a particular place or thing must be protected against warrantless governmental searches, unless they have voluntarily exposed their private materials to a third party.[65] Until recently, this rule has governed all searches, regardless of the nature of the place or thing to be searched.[66]

III. *CARPENTER V. UNITED STATES*

In 2018, the Supreme Court once again addressed the limits of the Fourth Amendment's protections in *Carpenter v. United States*.[67] In that case, police officers arrested four men who were suspected of robbing several RadioShack and T-Mobile stores between 2010 and 2012.[68] After one of the suspects confessed to committing the string of robberies, prosecutors obtained a court order under the Stored Communications Act to obtain the cell phone records of Carpenter.[69] Using this order, the FBI obtained 127 days of Carpenter's cell phone records, including the cell site location information (CSLI) for Carpenter over a four-month period.[70] The CSLI included

---

[62] Park, *supra* note 27, at 5 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018)).

[63] *Id.* at 11–12 (quoting *Carpenter*, 138 S. Ct. at 2216).

[64] *Id.* at 12.

[65] *See Smith*, 442 U.S. at 743–44 (explaining the Court's consistent holding that a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (citations omitted)).

[66] *See Carpenter*, 138 S. Ct. at 2215–17 (holding that the third-party doctrine did not extend to the collection of 127 days of cell site location information).

[67] *See id.* at 2217, 2221, 2223 (holding, narrowly, that an individual has a legitimate privacy interest in 127 days of cell site location information held by third parties, such that obtaining the location information from the defendant's wireless carrier constituted a search and required a warrant).

[68] Stephen E. Henderson, Carpenter v. United States *and the Fourth Amendment: The Best Way Forward*, 26 WM. & MARY BILL RTS. J. 495, 497 (2017).

[69] *Carpenter*, 138 S. Ct. at 2212. The Stored Communications Act allows the government "to compel the disclosure of certain telecommunications records" whenever it can provide "'specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id.* (quoting 18 U.S.C. § 2703(d)).

[70] *Id.* As the Court explained:

> Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell

12,898 location points,[71] showing the location of Carpenter's phone at the time of each incoming and outgoing call's origination and termination.[72]

Using the CSLI obtained from Carpenter's cell phone, the government was able to create maps showing Carpenter's proximity to the location of each of the known robberies at the time they were committed.[73] As a result of these maps and other related testimony, Carpenter was charged with and convicted of six counts of robbery and six counts of carrying a firearm during a federal crime of violence.[74] He was ultimately sentenced to over 100 years in prison.[75]

Prior to trial, Carpenter attempted to suppress the cell phone data by arguing that the seizure of his cell site location records constituted an unlawful search, as it was conducted without a warrant or probable cause.[76] The trial court denied Carpenter's motion to suppress, and the court of appeals affirmed the decision.[77] The Sixth Circuit concluded that Carpenter lacked a reasonable expectation of privacy in the location information collected by the government, as he had knowingly shared that information with his wireless cell phone carriers.[78] As such, the court held that the collection of data did not constitute a search.[79] The lower courts relied on the well-established third-party doctrine to reach their holdings, reasoning that the location data could be considered business records held by and obtained from a third-party phone company.[80]

The case then reached the Supreme Court, where the Justices considered whether the government conducts a search when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.[81] In a surprising

---

> sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.
>
> Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI).

Id. at 2211.

[71] *Id.* at 2212 (the 12,898 data points collected over the period of 127 days included "an average of 101 data points per day").

[72] *Id.*

[73] Henderson, *supra* note 68, at 497.

[74] *Carpenter*, 138 S. Ct. at 2212.

[75] Henderson, *supra* note 68, at 497.

[76] *Carpenter*, 138 S. Ct. at 2212.

[77] *Id.* at 2212–13.

[78] *Id.* at 2213.

[79] *Id.*; *see also* Henderson, *supra* note 68, at 502.

[80] *See* Henderson, *supra* note 68, at 502–03.

[81] *Carpenter*, 138 S. Ct. at 2211.

departure from the Court's third-party doctrine precedent, the Court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[82] The majority of the Court declined to extend the third-party doctrine to CSLI for two key reasons: first, that the exposure of such location data to a third-party wireless carrier is not "truly voluntary,"[83] and second, that this type of modern technology gave the government the unique ability to "chronicle a person's past movements through the record of his cell phone signals."[84]

The Court chose not to apply *Smith* and *Miller* to the collection of CSLI, noting that the exposure of such location data to some third party does not itself overcome a user's claim to Fourth Amendment protection.[85] The Court determined that the voluntary exposure rationale of the third-party doctrine was ill-suited to the collection of CSLI for several reasons.[86] First, they noted that cell phones have become "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[87] Second, cell phone users do not "voluntarily 'assume[] the risk'" of turning over their location information to a third party, as such information is automatically recorded by necessity of the operation of the cell phone itself, unless one turns off their cell phone entirely.[88] As such, the Court found it a mischaracterization to state that a cell phone user affirmatively and willingly chooses to give this information to a third party.[89]

Next, the Court expressed serious Orwellian concerns regarding the invasive nature of such location information and the ability of a 127-day record of CSLI to provide an all-encompassing record of a person's whereabouts.[90] Such a record necessarily "provides an intimate window into a person's life, revealing not only his particular movements,"[91] but the "privacies of life,"[92] including his "familial, political, professional, religious, and sexual associations,"[93] as evidenced by his daily locations.[94]

For these reasons, the Court noted that the collection of digital location tracking data over a prolonged period of time is distinct from the limited types of personal data obtained from third parties in *Smith* and *Miller*.[95] Thus, the government's argument that the collection of Carpenter's data "'turns on a garden-variety request

---

[82] *Id.* at 2217.
[83] *Id.* at 2219–20; *see also* Carthew, *supra* note 17, at 208.
[84] *Carpenter*, 138 S. Ct. at 2216.
[85] *Id.* at 2220.
[86] Park, *supra* note 27, at 12.
[87] *Id.* (quoting *Carpenter*, 138 S. Ct. at 2220).
[88] *See id.* (quoting *Carpenter*, 138 S. Ct. at 2220).
[89] *See id.*
[90] Carthew, *supra* note 17, at 210.
[91] *Carpenter*, 138 S. Ct. at 2217.
[92] *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)).
[93] *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).
[94] *Id.* at 2217.
[95] *See id.* at 2219.

for information from a third-party witness . . . fails to contend with the seismic shifts in digital technology' that include 'the exhaustive chronicle of location information casually collected by wireless carriers today.'"[96] The Court seemingly "found itself 'obligated . . . to ensure that the "progress of science" does not erode'" the protections afforded to individuals by the Fourth Amendment.[97] Finally, in light of the unique nature of CSLI, the Supreme Court held that the government will generally be required to obtain a warrant in order to access historical cell-site location information.[98]

The Court's holding in *Carpenter* resulted in a new balancing test, which weighs, on one hand, one's reasonable expectation of privacy with, on the other, whether the information was truly voluntarily exposed to a third party.[99] However, no broadly applicable principle emerged from the Court's opinion in *Carpenter*, leaving the breadth of the Court's holding as applied to other types of modern technology unknown.[100]

IV. FITBIT DEVICES AND THE POTENTIAL FOR USE OF ELECTRONIC FITNESS TRACKERS IN CRIMINAL INVESTIGATIONS AND PROSECUTIONS

A. The Capabilities of Fitbit Devices

Fitbits are physical activity tracking devices that are worn on one's wrist and can measure a person's heart rate, stress level, brain activity, respiration, and body temperature, among other things.[101] Fitbit was founded in 2007 and launched its first fitness tracker in 2009.[102] Today, Fitbit, Inc. sells four different fitness trackers and three smartwatches, each with its own unique function, capability, and style.[103]

Fitbits and other fitness trackers and smart-watches have become highly popularized, with 102.4 million devices sold in 2016 alone.[104] Fitbit devices accounted for almost twenty-two percent of the total devices shipped that year.[105] In fact, Fitbit, Inc. sold 22.3 million devices in 2016 and reported approximately 23.2 million active users.[106]

---

[96] Park, *supra* note 27, at 11 (alteration in original) (quoting *id.* at 2219).

[97] *Id.* at 12 (alteration in original) (quoting *Carpenter*, 138 S. Ct. at 2223).

[98] *Id.* at 5.

[99] Mary-Kathryn Takeuchi, *A New Third-Party Doctrine: The Telephone Metadata Program and* Carpenter v. United States, 94 NOTRE DAME L. REV. 2243, 2244 (2019).

[100] Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 235 (2019).

[101] Park, *supra* note 27, at 30.

[102] Carrie Marshall & James Stables, *The Story of Fitbit: How a Wooden Box Was Bought by Google for $2.1bn*, WAREABLE (Apr. 4, 2020), https://www.wareable.com/fitbit/story-of-fitbit-7936 [https://perma.cc/4QU6-2K8R].

[103] *See Products*, FITBIT, http://www.fitbit.com/global/us/products [http://perma.cc/H6Q6-RKKD] (last visited Dec. 8, 2020); *Home*, FITBIT, http://www.fitbit.com/home [http://perma.cc/6VT9-TZEA] (last visited Dec. 8, 2020).

[104] Kendall, *supra* note 15, at 335.

[105] *Id.* at 335–36 ("Apple made up approximately 10.5%, Garmin approximately 5.9%, and Samsung comprised around 4.3% of the total units shipped in 2016.").

[106] *Id.* at 336.

In order to use their products, Fitbit requires users to disclose their names, email addresses, dates of birth, genders, heights, and weights.[107] Fitbit also strongly recommends that users provide additional information such as daily food logs, sleep habits, water intake, and female health tracking in order to "improve [the user's] experience or enable certain features of the Services."[108] During use, the device collects data, such as the number of steps the user takes, their total distance traveled each day, calories burned, heart rate, sleep stages, and total active minutes.[109] Many of these features require use of "precise geolocation data, including GPS signals, device sensors, Wi-Fi access points, and cell tower IDs."[110] The Fitbit privacy policy notes that Fitbit, Inc. stores all information and data collected from use of its devices, *unless* the user deletes the data from their account.[111] However, it also notes that the deletion of such data would negatively impact the device's ability to provide the user with personal statistics and other aspects of the services.[112]

B. The Potential for Use of Electronic Fitness Trackers in Criminal Investigations and Prosecutions

The Fitbit privacy policy states:

> We may preserve or disclose information about you to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of the Services or the physical safety of any person.[113]

Because Fitbit collects and stores users' personal data, such data has the potential to be used by law enforcement.[114] Law enforcement officials have two potential

---

[107] *Fitbit Privacy Policy*, *supra* note 10 (stating that Fitbit uses "information like your height, weight, gender, and age" to "estimate a variety of metrics like the number of steps you take, your distance traveled, [and] calories burned").

[108] *Id.* ("Based on your sleep data, we may make inferences about your sleeping patterns and provide you with customized insights to help you improve your sleep. We may personalize exercise and activity goals for you based on the goals you previously set and your historical exercise or activity data.").

[109] *Id.*

[110] *Id.* ("When you allow us to collect precise location information, we use that information to provide and improve features of the Services such as recording where a workout took place or mapping an activity.").

[111] *See id.*

[112] *See id.*

[113] *Id.*

[114] *See* Henderson, *supra* note 68, at 510.

interests in using Fitbit data.[115] First, the government has an interest in using this data to solve past crimes.[116] Like in *Carpenter* where the government used 127 days of CSLI data to prove that the defendant was near the scene of each of the robberies during their commission, law enforcement could use the historical location information collected by Fitbit to pinpoint a user's location in order to prove or disprove their proximity to a crime scene during the commission of the crime.[117] The government's second potential interest in using Fitbit data is to prevent future crimes.[118] This interest could be achieved in one of two ways.[119] First, the collection of Fitbit data could have a general deterrence effect.[120] For example, if people knew that their location was being recorded and could later be used against them in a criminal prosecution, they might be less inclined to commit a crime for fear of being caught.[121] Second, real-time surveillance of users' data, including their locations, gives law enforcement the ability to intervene and prevent crimes from occurring when they suspect crime is afoot.[122]

Fitbit data is already being used by law enforcement in these ways across the country.[123] For example, in the investigation of Connie Dabate's murder in December 2015, Connecticut law enforcement officials used the victim's Fitbit data to reveal the time and location of her last recorded steps.[124] The data revealed that Connie Dabate's last movements inside her home were at approximately 10:05 a.m., about an hour after her husband, Richard Dabate, had told law enforcement officials that an armed intruder broke into their home and shot his wife.[125] In that case, the Fitbit data obtained by law enforcement was ultimately used to charge Richard Dabate with the first-degree murder of his wife.[126]

Alternatively, Fitbit data can been used to prove that a suspect in a criminal investigation was *not* responsible for the alleged crime.[127] In one case, for example, two young boys found the brutally beaten body of a woman, Nicole VanderHeyden, and reported it to the police.[128] Investigators initially suspected the woman's live-in

---

[115] *See id.*

[116] *Id.*

[117] *See* Carpenter v. United States, 138 S. Ct. 2206, 2212–13 (2018); *see also* Henderson, *supra* note 68, at 510.

[118] Henderson, *supra* note 68, at 510.

[119] *See id.*

[120] *Id.*

[121] *See id.*

[122] *Id.* at 511.

[123] *See* Kendall, *supra* note 15, at 337.

[124] *Id.* at 338; Altimari, *supra* note 4.

[125] *See* Altimari, *supra* note 4.

[126] *See* Paiella, *supra* note 5.

[127] *See* Kate Briquelet, *'My Fitbit Proves I Didn't Kill Her,'* DAILY BEAST (June 6, 2017, 8:50 AM), http://www.thedailybeast.com/my-fitbit-proves-i-didnt-kill-her [http://perma.cc/AJ9D-R456].

[128] *See id.*

boyfriend for her murder, but his Fitbit data ultimately revealed that he was asleep at home at the time of his girlfriend's death, thereby confirming his alibi and clearing him of any further suspicion by law enforcement.[129]

Finally, law enforcement officials have used Fitbit data to confirm or deny victims' stories regarding alleged attacks.[130] In one case, police used an alleged victim's own Fitbit data to determine that her police report, claiming that she had been forced out of her bed and raped, was false, and that instead, she had walked around all night staging a crime scene in her home.[131] Police also used Fitbit location information to confirm the report of a jogger who reported she was attacked in Seattle while on a run.[132] In that case, law enforcement officials used the victim's Fitbit data to track the route of her run, then overlaid an aerial photograph of the area to determine where the attack occurred.[133]

These examples demonstrate only a few of the ways in which Fitbit data has the potential to be used by law enforcement in criminal investigations and prosecutions.[134] Experts in the field suggest that the use of Fitbit data in criminal prosecutions will only become more popular over time.[135] In fact, a state police special agent in the high technology division suggested that such evidence "will definitely be something in five or [ten] years, in every case, [that the police] will look to see if this information is available."[136] Therefore, because of the popularity of Fitbit devices, the sensitive nature of the information stored on such devices, and their potential use in criminal investigations and prosecutions, it is necessary to determine whether the collection of data from a Fitbit constitutes a search and, if so, whether such a search requires a warrant.

V. ANALYSIS: IN LIGHT OF *CARPENTER V. UNITED STATES*, THE COLLECTION OF FITBIT DATA BY LAW ENFORCEMENT SHOULD BE CONSIDERED A SEARCH AND REQUIRE A WARRANT UNDER THE FOURTH AMENDMENT

The Court's holding in *Carpenter* regarding the collection of 127 days of CSLI should be extended to govern the collection of Fitbit data so that the government's collection of seven or more days of Fitbit data constitutes a search under the Fourth Amendment and law enforcement are required to obtain a warrant before collecting

---

[129] *See id.*

[130] *See* Kendall, *supra* note 15, at 337–38.

[131] *See id.*

[132] *See id.* at 338.

[133] *See id.*

[134] *See id.* at 337–38.

[135] *See* Justin Jouvenal, *Commit a Crime? Your Fitbit, Key Fob or Pacemaker Could Snitch on You*, WASH. POST (Oct. 9, 2017), http://www.washingtonpost.com/local/public-safety/commit-a-crime-your-fitbit-key-fob-or-pacemaker-could-snitch-on-you/2017/10/09/f35a4f30-8f50-11e7-8df5-c2e5cf46c1e2_story.html [http://perma.cc/8PBR-PNKY].

[136] *Id.*

such data for use in criminal investigations or prosecutions.[137] The extension of *Carpenter*'s holding to the collection of Fitbit data is logical in light of the Court's analysis that the third-party doctrine is ill-suited to the digital age.[138] Such an extension is necessary to safeguard the protections of the Fourth Amendment in the twenty-first century. Finally, such an extension is realistic in light of the Court's other recent Fourth Amendment precedent.

A. Before Carpenter*, the Collection of Fitbit Data by Law Enforcement Would Not Have Constituted a Search Under the Third-Party Doctrine*

Before *Carpenter*, the question of whether the collection of Fitbit data by law enforcement for use in a criminal prosecution constitutes a search under the Fourth Amendment would be a simple one. The answer would be a resounding 'no,' under the Supreme Court's well-established Fourth Amendment precedent, including the *Katz* reasonable expectation of privacy test and the third-party doctrine.[139]

Because the collection of Fitbit data does not require law enforcement officials to *physically* trespass into a constitutionally protected area,[140] the Supreme Court would have almost certainly relied upon the *Katz* reasonable expectation of privacy test to determine whether the collection of such data constitutes a search under the Fourth Amendment prior to its decision in *Carpenter*.[141] Although the Court may have determined that a Fitbit user maintains a subjective expectation that their personal health, fitness, and location data, including their steps taken, heart rate, and calories burned, among other data, would be kept private, the Court would have likely found this expectation was one that society is not prepared to recognize as reasonable under the second prong of the *Katz* test.[142]

Under the third-party doctrine, the Court would have likely found that a Fitbit user does not have a reasonable expectation of privacy in the data stored on their device.[143] The Court would likely have reasoned that, much like the financial records disclosed to the bank in *United States v. Miller*[144] and the phone numbers disclosed to the telephone company in *Smith v. Maryland*,[145] one who wears a Fitbit device lacks a

---

[137] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217, 2220–21 (2018).

[138] *See id.* at 2216–21.

[139] *See* United States v. Miller, 425 U.S. 435, 443 (1976); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[140] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

[141] *See Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[142] *See id.*; *Fitbit Privacy Policy*, *supra* note 10. The *Katz* test is comprised of two unique, but related requirements: "first[,] that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[143] *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1979); *Miller*, 425 U.S. at 442.

[144] *See* 425 U.S. at 436.

[145] *See* 442 U.S. at 742.

reasonable expectation of privacy in such data, as they have voluntarily disclosed their personal information to a third party, namely Fitbit, Inc.[146] Holding that the individual lacked a reasonable expectation of privacy, the Court would have determined that obtaining Fitbit data did not constitute a search.[147] Thus, under the Supreme Court's pre-*Carpenter* precedent, the government would be free to obtain such information from Fitbit, Inc. without a warrant and without violating the Fourth Amendment.[148]

B. In Light of Carpenter v. United States*, the Collection of Fitbit Data by Law Enforcement Should Be Considered a Search, as the Third-Party Doctrine Is Ill-Suited to the Digital Age*

While the question of whether the collection of Fitbit data constitutes a search would previously have been easily resolved by the *Katz* test and the third-party doctrine, the Supreme Court's recent holding in *Carpenter v. United States* suggests that the third-party doctrine may no longer be the appropriate test by which to answer this inquiry.[149] Although the Court's decision in *Carpenter* was limited to the collection of the 127 days of CSLI involved in that particular case, the Court's reasoning that the third-party doctrine is ill-suited to modern technology is widely applicable to numerous types of technology, including Fitbit data.[150]

1. Fitbit Data, like CSLI, Is Not Truly "Voluntarily" Exposed to Third Parties

In reaching the determination that the collection of CSLI constituted a search, the Court relied on two main arguments: First, the Court reasoned that CSLI is not truly "voluntarily exposed" to telephone companies, because disclosure of data is "incidental to merely having a cell phone, an item necessary for functioning in modern society."[151] Emphasizing the pervasiveness of cell phones in today's world to demonstrate the lack of choice one has in exposing such data to third parties, Justice Sotomayor commented during the November 2017 oral arguments for *Carpenter* that many people carry their cell phones with them almost 24/7, even "into their beds and public restrooms."[152] In fact, Justice Sotomayor noted that cell phones are "an appendage now for some people."[153]

---

[146] *See id.*; Takeuchi, *supra* note 99, at 2243.

[147] *See Katz*, 389 U.S. at 353.

[148] *See* Park, *supra* note 27, at 5.

[149] *See* 138 S. Ct. 2206, 2219–20 (2018).

[150] *See* Park, *supra* note 27, at 28–29.

[151] *Id.* at 1, 11–12.

[152] *Id.* at 1; *see also* Transcript of Oral Argument at 42–43, *Carpenter*, 138 S. Ct. 2206 (No. 16-402).

[153] Park, *supra* note 27, at 1 (quoting Greg Stohr, *Supreme Court Justices Hint at More Digital-Privacy Protections*, BLOOMBERG, http://www.bloomberg.com/news/articles/2017

If Justice Sotomayor is correct that cell phones have become indispensable to daily functioning in modern life, then certainly the same can be said for Fitbits.[154] In fact, Fitbits "are perhaps *more* likely to be found on the person, as they are designed to be worn on the body as an armband."[155] Furthermore, like the telephone companies' automatic collection and storing of the CSLI at issue in *Carpenter*, Fitbit, Inc. stores its users' data, including their health and location information, automatically, *unless* the user manually deletes the data from their account settings.[156] Although one might argue that users voluntarily disclose such data to Fitbit, Inc., a third party, when they agree to the terms of service provided by the company in order to use their devices, it is no secret that most users do not take the time to read the terms of service or privacy policies upon receiving their new devices.[157] In fact, most people "quickly tap 'next,' 'next', [sic] and 'Agree,'" to the long list of small-font terms listed.[158] Thus, it is hardly fair to say that users affirmatively "opt in" to sharing their personal data with Fitbit, Inc.[159]

Moreover, even if a user *wanted* to opt out of sharing their personal data with Fitbit, doing so would limit the functioning abilities of the device, thereby providing a disincentive for users to opt out of sharing this information.[160] Fitbit users, like cell phone users, cannot be said to "voluntarily" expose their health and location data to a third party through mere use of a Fitbit device.[161] As such, like in *Carpenter*, the "voluntary exposure" rationale of the third-party doctrine is ill-suited to the collection of Fitbit data.[162]

2. The Collection of Fitbit Data Constitutes a "Seismic Shift" in Technology Not Contemplated by the Third-Party Doctrine

The Court in *Carpenter* reasoned that the third-party doctrine was inapplicable to the collection of 127 days of CSLI because such a vast amount of location data gave the government the unique ability to "chronicle a person's past movements

---

-11-29/supreme-court-justices-hint-at-new-digital-privacy-protections [http://perma.cc/B26P-LTS5] (Nov. 29, 2017, 2:57 PM)).

[154] *See id.*

[155] Katharine Saphner, Note, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1711 (2016) (emphasis added).

[156] *See Fitbit Privacy Policy*, *supra* note 10.

[157] *See* Sophie Charara & Husain Sumra, *We Read Your Wearable Tech's Privacy Policy So You Don't Have to*, WAREABLE (May 25, 2018), http://www.wareable.com/wearable-tech/terms-and-conditions-privacy-policy-765 [http://perma.cc/T3ER-P7X2].

[158] *Id.*

[159] *See id.*

[160] *See Fitbit Privacy Policy*, *supra* note 10 (The Fitbit, Inc. privacy policy states that the company collects and stores users' information because such data is necessary to providing users with personal statistics and other aspects of the services Fitbit devices offer.).

[161] *See generally id.*

[162] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

through the record of his cell phone signals," thereby revealing the intimate details of one's life.[163] The same can be said for the collection of Fitbit data. In fact, Fitbit data may be even *more* sensitive and revealing than CSLI alone.[164] "While cell phones are designed to communicate with the outside world, activity trackers are designed to collect data about the way users live their lives, and then display it back to the user."[165] Fitbit tracks not just one's approximate location based on CSLI, but also a user's exact locations, the number of steps taken each day, their heart rate, sleep habits, stress level, brain activity, respiration, body temperature, food and water intake, and even female health information.[166] This kind of information provides an "intimate window into a person's life," by revealing what they eat, how they sleep, where they spend their time, and even their current state of health.[167] As such, the Court's reasoning for declining to apply the third-party doctrine to the kind of sensitive and revealing information at issue in *Carpenter* applies even more fervently to Fitbit data, as this type of data represents just the kind of "seismic shifts in digital technology" the Court expressed concerns about in *Carpenter*.[168]

Because the third-party doctrine should not apply to the collection of Fitbit data and the collection of such data infringes on a user's reasonable expectation of privacy, it must be considered a search under the Fourth Amendment. Warrantless searches are considered per se unreasonable under the Fourth Amendment, subject to only a few, limited exceptions.[169] Thus, law enforcement should be required to obtain a warrant before collecting a user's Fitbit data.

C. Proposed Rule: Expanding Carpenter*'s Rationale to Provide a Generally Applicable Framework for Determining Whether the Collection of Data Constitutes a Search*

Going forward, courts should apply the *Carpenter* rationale to other types of technology to determine whether the collection of such data constitutes a search and requires a warrant under the Fourth Amendment. Where (1) the data contains "sensitive information" that has the potential to reveal the "privacies of [one's] life,"[170] (2) the

---

[163] *See id.* at 2216–20.

[164] *See* Nicole Chauriye, Note, *Wearable Devices as Admissible Evidence: Technology Is Killing Our Opportunities to Lie*, 24 CATH. U. J.L. & TECH. 495, 527 (2016); Park, *supra* note 27, at 30.

[165] Saphner, *supra* note 155, at 1714.

[166] *See* Kendall, *supra* note 15, at 337; Park, *supra* note 27, at 30; *Fitbit Privacy Policy*, *supra* note 10.

[167] *Carpenter*, 138 S. Ct. at 2217; *Fitbit Privacy Policy*, *supra* note 10.

[168] *Carpenter*, 138 S. Ct. at 2219; Park, *supra* note 27, at 11.

[169] Katz v. United States, 389 U.S. 347, 357 (1967). Whether the collection of Fitbit data would fall within one such exception to the general warrant requirement is outside the scope of this Note.

[170] *Carpenter*, 138 S. Ct. at 2214, 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

disclosure of such information is not truly voluntarily, but rather merely incidental to the use of the technology itself, and (3) the use of such technology is necessary for functioning in modern society,[171] the collection of such data should constitute a search and require a warrant.

Although the Supreme Court's decision in *Carpenter* was limited to holding that 127 days of CSLI, which included 12,898 location points, constituted a search,[172] the Court's reasoning suggests that the rule should not be limited to applying only to the collection of such a lengthy period of data.[173] In *Carpenter*, the Court noted that the 127 days of CSLI constituted a search because it provided law enforcement with a comprehensive chronicle of the user's past movements.[174] The 12,898 location points obtained in *Carpenter* came from location transmissions providing the user's location at the time of the start and end of each call placed or received on his cell phone.[175]

Modern, wearable technological devices, such as Fitbits, track the wearer's location *constantly*, gathering and collecting data on the user's movements throughout the day, even when the user is not actively using the device's functions.[176] As such, Fitbits and other similar devices can easily collect 12,898 location points from a user in just a matter of days, as compared to the more than four months it took to gather this amount of data in *Carpenter*.[177]

For these reasons, the Supreme Court should adopt a rule wherein the collection of seven or more days of one's Fitbit data constitutes a search and requires a warrant.[178] The quantity and specificity of the location data collected by Fitbit devices over the course of a week is capable of revealing the same "privacies of [one's] life"[179] as the 127 days of CSLI in *Carpenter* by revealing "one's intimate relationships, hobbies, predilections, medical conditions, religious beliefs, and political pursuits"[180] through their location and health data.

---

[171] *See* Park, *supra* note 27, at 12.

[172] *See Carpenter*, 138 S. Ct. at 2212, 2220.

[173] *See id.* at 2219–20.

[174] *See id.* at 2218–19.

[175] *See id.* at 2211–12, 2217.

[176] *See Fitbit Privacy Policy*, *supra* note 10 ("The Services include features that use precise geolocation data, including GPS signals, device sensors, Wi-Fi access points, and cell tower IDs.").

[177] *See id.*

[178] This proposed "one week" rule should also apply to devices and technologies similar to Fitbits in their capabilities to constantly track a user's location even when the device is not actively being used. The collection of one week or more of data from any such device capable of tracking the entirety of one's movements during a particular day should thus constitute a search and require a warrant under the Fourth Amendment.

[179] *See Carpenter*, 138 S. Ct. at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

[180] Brief of Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae in Support of Petitioner at 4, *id.* (No. 16-402) [hereinafter Scholars' Brief].

D. Providing a Workable Standard for Data Collection Under the Fourth Amendment: Why Holding that the Collection of Fitbit Data Constitutes a Search and Requires a Warrant Is Both Necessary and Realistic

Holding that the collection of Fitbit data constitutes a search and requires a warrant under the Fourth Amendment is both necessary and realistic. As discussed hereinafter, the proposed rule is both consistent with the Framers' intent for the scope of the individual protections under the Fourth Amendment and necessary in order to protect against the dangers of an Orwellian state.[181] It is also necessary in order to provide law enforcement a bright-line rule.[182] Finally, this proposed rule is realistic in light of several practical considerations that suggest the Supreme Court's willingness to depart from the third-party doctrine.[183]

1. The Proposed Rule Is Consistent with the Framers' Intent for Individual Protections Under the Fourth Amendment

Holding that the government's collection of an individual's Fitbit data constitutes a search is consistent with the Framers' original intent for the scope of the protections under the Fourth Amendment.[184] The Fourth Amendment states,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[185]

At the time the Fourth Amendment was ratified, "to 'search' meant to 'examine,' 'explore,' 'look through,' 'inquire,' 'seek,' or 'try to find.'"[186] As such, although the Framers could not have imagined that the government would be able to collect records of one's past location data from a device worn on one's wrist, the collection of such data clearly constitutes a "search" under the original definition of the word.[187]

Furthermore, Fitbit location data implicates the same type of expressive and association activities that the Framers intended the Fourth Amendment to protect.[188]

---

[181] *See infra* Sections V.D.1 and V.D.2.

[182] *See infra* Section V.D.3.

[183] *See infra* Section V.D.4.

[184] *See* Scholars' Brief, *supra* note 180, at 2.

[185] U.S. CONST. amend. IV.

[186] Scholars' Brief, *supra* note 180, at 2 (quoting SAMUEL JOHNSON, A DICTIONARY OF THE ENGLISH LANGUAGE (10th ed. 1792)).

[187] *See id.* at 3.

[188] Brief of Amici Curiae Electronic Frontier Foundation, Brennan Center for Justice, the Constitution Project, National Ass'n of Criminal Defense Lawyers & National Ass'n of Federal

By including "papers" among the other places and things protected by the Amendment, the Framers clearly indicated that the Fourth Amendment's protection was meant to safeguard one's personal information from unreasonable searches and seizures by the government.[189] In fact, the Bill of Rights itself was created "against the background of knowledge that unrestricted power of search and seizure" could be dangerous to one's freedom of expression.[190] Thus, the collection of Fitbit data implicates the same type of information that the Framers intentionally set out to protect from warrantless governmental intrusions.[191]

The Framers chose the language of the Fourth Amendment carefully in order to shield against the types of invasions suffered by the Founding Fathers under Britain's writs of assistance.[192] In fact, the Framers believed that discretionary, arbitrary, and unfettered governmental power was inherently "unreasonable" and "against the reason of the common law" because of "its oppressive impact on 'the people' as a whole."[193] Although the Framers could not have anticipated the types of modern technological issues the Supreme Court is faced with today, "they would have recognized the dangers inherent in any [governmental] claim of unlimited authority to conduct searches for evidence of criminal activity."[194] Thus, holding that the collection of Fitbit data constitutes a search is consistent with the Framers' intent for the extent of the safeguards of the Fourth Amendment.

2. The Proposed Rule Is Necessary to Shield Against an "Orwellian State"

Concluding that the collection of Fitbit data constitutes a search and requires a warrant under the Fourth Amendment is the necessary rule "to ensure that the 'progress of science' does not erode Fourth Amendment protections."[195] Justice Sotomayor, in her concurrence in *United States v. Jones* stated:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital

---

Defenders in Support of Petitioner at 26, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402).

[189] *Id.*

[190] *Id.* (quoting Marcus v. Search Warrants of Prop. at 104 E. Tenth St., 367 U.S. 717, 729 (1961)).

[191] *See id.* at 28.

[192] Scholars' Brief, *supra* note 180, at 3 (the writs of assistance were a type of general warrant that allowed state agents to exercise broad discretion to search one's property with unbridled discretion).

[193] *Id.* (quoting Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1270 (2016)).

[194] *Id.* at 4.

[195] Park, *supra* note 27, at 12 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018)).

> age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[196]

Justice Sotomayor's concerns closely resemble the Court's later decision in *Carpenter*.[197] Other reasons exist why the Court's "1970s-era limited third party doctrine should [not] apply to twenty-first century technologies," including first and foremost that the doctrine appears to be "contrary to prevailing theories of information privacy."[198]

> To begin with, both the common law and the liberal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public."[199]

If a contrary rule regarding Fitbit data were adopted, allowing the government to access, collect, and use such data at its discretion, it would seriously undermine society's conception of privacy and would start society down a dangerous path to an Orwellian state.[200] "In a world of truly ubiquitous connectivity where we are recording our heartbeat, our steps, our location . . . if all of that data is now available to law enforcement without a warrant . . . that's a big invasion of what most of us think our privacy should include."[201] In fact, as Justice Sotomayor noted, these developments, if left unchecked, will "alter the relationship between citizen and government in a way that is inimical to democratic society."[202]

---

[196] United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (citations omitted).

[197] *See Carpenter*, 138 S. Ct. at 2220.

[198] Henderson, *supra* note 68, at 504.

[199] *Id.* at 505 (quoting U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press, 498 U.S. 749, 763 (1989)).

[200] *See* Carthew, *supra* note 17, at 210.

[201] Jouvenal, *supra* note 135 (first omission in original).

[202] United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

Although some may argue that the collection of Fitbit data is necessary to ensure the effectiveness of modern law enforcement, "[w]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement."[203] As technology continues to advance and "seismic shifts in digital technology" become a normality, the Court must be prepared to safeguard the protections of the Fourth Amendment more fiercely than ever before.[204]

3. The Proposed Rule Is Best Suited to the Protection of Individual Rights, as Law Enforcement Officials Need a Bright-Line Rule Regarding the Collection of Fitbit Data

Law enforcement officials need easily applied rules regarding collection of Fitbit data.[205] In fact, the Court's Fourth Amendment jurisprudence has consistently emphasized the importance of the workability of the rules law enforcement officials must follow.[206] This is because police decisions are often "quick ad hoc judgment[s]."[207] In *Riley*, for example, the Court emphasized the need for easily applicable rules in the context of police investigations, stating that "[i]f police are to have workable rules, the balancing of the competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[208] As such, a bright-line rule requiring police to obtain a warrant before collecting Fitbit data is best suited to safeguard individuals' Fourth Amendment protections.

4. Several Practical Considerations Suggest the Supreme Court's Willingness to Depart from the Third-Party Doctrine

Finally, several practical considerations suggest that the Supreme Court may be willing to depart from the third-party doctrine, especially in cases involving modern technology.[209] First, there is reason to believe that the Supreme Court no longer supports the doctrine.[210] The Court has not applied the doctrine in several decades, suggesting its reluctance to reaffirm the doctrine in a modern context.[211] Moreover, none of the current Supreme Court justices were on the bench at the time the Court last applied the third-party doctrine.[212]

---

[203] GRONLUND, *supra* note 1, at 204.
[204] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
[205] *See* Riley v. California, 573 U.S. 373, 396–400 (2014).
[206] *See* Saphner, *supra* note 155, at 1718.
[207] *Id.* (alteration in original) (quoting United States v. Robinson, 414 U.S. 218, 235 (1973)).
[208] *Id.* (omissions in original) (quoting *Riley*, 573 U.S. at 398).
[209] *See* Henderson, *supra* note 68, at 504.
[210] *Id.*
[211] *Id.*
[212] *Id.*

Second, recent Supreme Court precedent regarding the application of the warrant requirement under the Fourth Amendment suggests the Court recognizes that many of its previously well-established precedents regarding Fourth Amendment protections may be ill-suited in application to advanced technology in the digital age.[213] For example, in *Riley v. California*, the Court held that the search incident to arrest exception to the warrant requirement under the Fourth Amendment does not apply to searches of cell phones incident to arrest because of the uniquely private nature of cell phones.[214]

Prior to the Court's decision in *Riley*, the general rule, expressed in *United States v. Robinson*, was that a search of an arrestee's person incident to a lawful custodial arrest "require[d] no additional justification," other than the arrest itself.[215] In that case, the search incident to arrest doctrine allowed police officers to conduct a pat-down of arrestee Robinson.[216] During the search, the officers felt an unidentified object that later turned out to be a cigarette package in his coat pocket which they subsequently removed and opened to find fourteen capsules of heroin.[217]

In *Riley*, the Court recognized that the search of one's cell phone is significantly more intrusive than "the type of brief physical search considered in *Robinson*."[218] The Court noted that a search of one's cell phone, unlike the search of one's pockets, has the potential to reveal large quantities of personal data.[219] In fact, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[220]

The Court discussed at length the numerous ways in which cell phones differ both quantitatively and qualitatively from other objects that might typically be found during a search incident to an arrest, in order to explain why the search incident to arrest doctrine is ill-suited to such modern technology.[221] For example, the Court

---

[213] *See Riley*, 573 U.S. at 392–93 (distinguishing cell phone searches from other searches incident to arrest because they "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse").

[214] *Id.* at 386 ("Cell phones . . . place vast quantities of personal information literally in the hands of individuals. . . . We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

[215] 414 U.S. 218, 235 (1973).

[216] *Id.* at 221–22.

[217] *Id.* at 223.

[218] *Riley*, 573 U.S. at 386. The Court in *Riley* expressed its strong disagreement with the government's assertion that the search of all data stored on a cell phone could be considered "materially indistinguishable" from searches of physical items. *Id.* at 393 (quoting Brief for the United States as Amicus Curiae Supporting Respondent at 26, *id.* (No. 13-132)). In fact, the Court stated that such a claim "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Id.*

[219] *Id.* at 386.

[220] *Id.* at 393.

[221] *Id.* at 393–96.

found the "immense storage capacity" of modern cell phones problematic under the search incident to arrest doctrine.[222] The Court noted that the search incident to arrest doctrine was created to allow only for a *narrow* intrusion of privacy, as most people cannot and do not attempt to physically carry "every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read."[223] Thus, a search of one's person incident to arrest prior to the advent of cell phones was relatively limited in its breadth.[224]

In contrast, the Court noted that cell phones' large storage capacity makes it possible for people to carry with them hundreds or even thousands of emails, photos, videos, text messages, internet browsing histories, calendar events, and phone book entries at all times.[225] The Court expressed its concern that, taken together, this information can reveal far more information than previously possible during a search incident to an arrest, as "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."[226]

Thus, because of the large quantity of uniquely sensitive information "from the mundane to the intimate" that is often stored on one's cell phone, the Court in *Riley* declined to apply the search incident to arrest exception to the warrant requirement to cell phone searches.[227] The Court held instead that law enforcement officers are required to obtain a warrant before searching a cell phone incident to an arrest.[228]

The Court's decision in *Riley*, though not readily applicable to the collection of Fitbit data for use in criminal investigations, demonstrates the Supreme Court's willingness to depart from its established rules and doctrines regarding the reasonableness of searches under the Fourth Amendment when modern technologies are involved.[229] *Riley* also illustrates the Court's recognition of the unique nature of modern technology and the privacy interests at stake when police gain access to large amounts of such personal data.[230] In fact, the Court's concerns regarding the storage capacity of modern devices and the potential for the data stored on such devices to reconstruct "[t]he sum of an individual's private life"[231] can easily be applied to the collection of data from Fitbits, as such devices share cell phones' ability to store intimate details related to one's personal life.[232]

---

[222] *Id.* at 393.
[223] *Id.* at 393–94.
[224] *Id.* at 393.
[225] *See id.* at 394.
[226] *Id.*
[227] *Id.* at 393, 395.
[228] *Id.* at 403.
[229] *See generally id.*
[230] *See generally id.*
[231] *See id.* at 394.
[232] *See Fitbit Privacy Policy*, *supra* note 10.

For this reason, it is reasonable to believe that the Supreme Court, having not applied the third-party doctrine in several decades and having since recognized other Fourth Amendment doctrines as incompatible with modern technologies, would be willing to extend *Carpenter v. United States* and find the third-party doctrine inapplicable to the collection of Fitbit data.[233]

CONCLUSION

Although Fitbit data has the potential to be extremely useful to law enforcement officials in criminal investigations and prosecutions in the future, "[w]e cannot forgive the requirements of the Fourth Amendment in the name of law enforcement."[234] Because of the popularity of Fitbit devices in our modern, technology-dependent world, the sensitive nature of the personal location and health information stored on these devices,[235] and their potential use in criminal investigations and prosecutions, the Court must exercise due care when considering whether the collection of such data constitutes a search under the Fourth Amendment.

The collection of seven or more days of data from a user's Fitbit by law enforcement should be considered a search under the Fourth Amendment, and should require a warrant. The previously controlling third-party doctrine is ill-suited to the digital age, as suggested by the Court's recent decision in *Carpenter v. United States*.[236] Requiring law enforcement officials to obtain a warrant prior to collecting such data both reflects the Framers' original intentions for the protections afforded to individuals by the Fourth Amendment, and "ensure[s] that the 'progress of science' does not erode Fourth Amendment protections."[237] Furthermore, a bright-line, categorical warrant rule governing the collection of Fitbit data is necessary to safeguard individuals' Fourth Amendment protections, as decisions by law enforcement officers are often made using "quick ad hoc judgments."[238] Finally, the Court's recent willingness to depart from previously well-established Fourth Amendment doctrines when it encounters "seismic shifts in digital technology," reflects the Court's recognition of the unique nature of modern technology and its need for differing treatment under the law.[239]

For these reasons, the collection of seven or more days of Fitbit data by law enforcement should not be analyzed under the third-party doctrine. Instead, the Court should extend *Carpenter*'s holding to apply to the collection of Fitbit data, as

---

[233] *See* 138 S. Ct. 2206, 2220 (2018); *Riley*, 573 U.S. at 403.

[234] GRONLUND, *supra* note 1, at 204.

[235] *See Fitbit Privacy Policy*, *supra* note 10.

[236] *See Carpenter*, 138 S. Ct. at 2216–20.

[237] Park, *supra* note 27, at 12 (quoting *id.* at 2223).

[238] Saphner, *supra* note 155, at 1718 (quoting United States v. Robinson, 414 U.S. 218, 235 (1973)).

[239] *See Carpenter*, 138 S. Ct. at 2219.

well as other sensitive, personal, and location-based technology, and should require police to obtain a warrant before collecting more than one week's worth of such data, as such a span of sensitive information has the dangerous potential to reveal the intimate details of one's life.[240] In the future, the Court should analyze new technologies under the *Carpenter* rationale to determine whether the collection of data from such devices constitutes a search.[241] Where (1) the data contains "sensitive information" that has the potential to reveal the "privacies of [one's] life,"[242] (2) the disclosure of such data is not truly voluntary, but rather merely incidental to the use of the technology itself, and (3) the use of such technology is necessary for functioning in modern society,[243] the collection of data should constitute a search and require a warrant.

---

[240] *See id.* at 2220.
[241] *See generally id.*
[242] *Id.* at 2217 (quoting Riley v. California, 573 U.S. 373, 403 (2014)).
[243] Park, *supra* note 27, at 12.